AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: Mark R. Stoneman, 6/6/2023

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)
)
)
a 2013 Silver Dodge Dart, bearing Oklahoma)
Comanche Nation license plate number CN3060)

Case No: M-23-450-AMG

APPLICATION FOR SEARCH WARRANT

I, Jesse M. Stoda, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

Located in the Western District of Oklahoma, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1111 and 1152	First-Degree Premeditated Murder,

The application is based on these facts:

See attached Affidavit of Special Agent Jesse M. Stoda, FBI, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Jesse M. Stoda
Special Agent
FBI

Sworn to before me and signed in my presence.

Date: 6/7/23

Judge's signature

City and State: Oklahoma City, Oklahoma

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Jesse M. Stoda, a Special Agent of the Federal Bureau of Investigation (FBI), Oklahoma City Division, being duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent with the FBI since July 2017 and have been assigned to the Oklahoma City Division of the FBI for approximately 2 years. During the past 6 years, I have conducted a wide variety of investigations, including cases involving violent crimes in Indian country.

2. I have personally participated in the investigation set forth below. The facts in this Affidavit come from my personal observations, my review of documents related to this investigation, oral and written communications with others who have personal knowledge of the events and circumstances described herein, a review of public source information including information available on the Internet, my training and experience, and information obtained from other agents and witnesses.

3. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

4. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of Title 18, United States Code, Sections 1111 and 1152 are located within a 2013 Silver Dodge Dart, bearing Oklahoma Comanche Nation license plate number CN3060 (the "**SUBJECT VEHICLE**"), including

all digital devices therein. I submit this Application and Affidavit in support of a search warrant authorizing a search of the **SUBJECT VEHICLE**, as further described in Attachments A and B, incorporated herein by reference, which is located in the Western District of Oklahoma. Located within the **SUBJECT VEHICLE** to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire **SUBJECT VEHICLE**, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

5. Further, I believe there is probable cause to search the digital devices that may be located in the **SUBJECT VEHICLE**, including computers, mobile phones, and/or tablets, hereinafter the "digital devices," that such digital devices will contain evidence, instrumentalities, and contraband of the crime. In support thereof, I state as follows:

PROBABLE CAUSE

6. On May 17, 2023, a woman later identified by the initials K.S.C.[1] was found dead in the Wichita Mountains Wildlife Refuge in Oklahoma. K.S.C. possessed Indian blood and is an enrolled tribal member with the Comanche Nation. K.S.C. appeared to have suffered bludgeon wounds to her face and head.

7. On May 19, 2023, investigators searched K.S.C.'s home. Inside the home, investigators observed blood consistent with a violent struggle. K.S.C.'s vehicle, a 2013 Silver Dodge Dart, bearing Oklahoma Comanche Nation license plate number CN3060,

1 The identity of K.S.C. is known to the FBI.

the **SUBJECT VEHICLE**, was missing from her home. K.S.C.'s home is located in Lawton, Oklahoma, and is on land within the Western District of Oklahoma that is held in trust under jurisdiction of the United States Government and qualifies as Indian Country under 18 U.S.C. § 1151(c) as an Indian allotment.

8. On May 21, 2023, law enforcement observed the **SUBJECT VEHICLE** driving south of Dallas, Texas. Law enforcement attempted to make a traffic stop on the vehicle. However, the vehicle did not pull over and instead attempted to flee at a high speed. Law enforcement pursued the vehicle until K.S.C.'s vehicle crashed into a small body of water just west of 2868 FM 1129, Powell, Texas, 75153. The occupants of the vehicle, SEMIEN and INDIVIDUAL 1 attempted to flee on foot but were ultimately apprehended and taken into custody by local law enforcement officers. Neither SEMIEN nor INDIVIDUAL 1 had mobile telephones on them when they were taken into custody.

9. Later that morning, the **SUBJECT VEHICLE** was towed from the crash site to a secure parking lot at Rice Police Department, located at 305 North Dallas Street, Rice, Texas 75165. A Rice Police Department officer escorted the tow truck during the transport.

10. On May 21, 2023, investigators interviewed SEMIEN who waived his *Miranda* rights and agreed to answer questions. At first, SEMIEN denied involvement in K.S.C.'s death. However, he eventually admitted that he had killed K.S.C. SEMIEN told investigators that INDIVIDUAL 1 is his girlfriend and a relative of K.S.C. SEMIEN said that INDIVIDUAL 1 asked him to kill K.S.C. because INDIVIDUAL 1 was angry with K.S.C. SEMIEN said that he was not sure INDIVIDUAL 1 was serious in her request, but she continued to ask SEMIEN to kill K.S.C. SEMIEN confessed that he eventually agreed

to kill K.S.C. He stated they both went to K.S.C.'s home where SEMIEN bludgeoned K.S.C. to death with a brick, then they left the area. Both SEMIEN and INDIVIDUAL 1 returned later that night, put her body in the trunk of the **SUBJECT VEHICLE**, and disposed of her body in the Wichita Mountains Wildlife Refuge.

11. On May 21, 2023, **SUBJECT VEHICLE** was towed from Rice Police Department to a secure parking lot at the Dallas FBI field office, located at 1 Justice Way, Dallas, Texas 75220. I escorted the tow truck during the transport.

12. On May 24, 2023, a seizure warrant was obtained for the **SUBJECT VEHICLE** to bring the vehicle from the Northern District of Texas back into the Western District of Oklahoma.

13. The **SUBJECT VEHICLE** is currently located at the Oklahoma City FBI Field Office within the Western District of Oklahoma.

14. I know from my training and experience that people commonly possess "smartphones," or mobile telephones that have the ability to access the internet and operate mobile applications. Smart phones are digital devices that operate in the same manner as a computer. Smart phones also have the ability to search the internet and save the history of these searches on the phone. I know through my training and experience that people tend to keep their smart phones on their person or within arm's reach of their person. Based on the statements of SEMIEN, it is likely that evidence concerning SEMIEN and INDIVIDUAL 1's state of mind, opportunity, preparation, plan, knowledge, or intent are likely to be found on digital devices in the **SUBJECT VEHICLE.**

15. Based on SEMIEN's statements about transporting K.S.C.'s body in the trunk of the **SUBJECT VEHICLE**, it is also likely that biological evidence related to K.S.C.'s death will be found within the **SUBJECT VEHICLE.**

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

i. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

b. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

c. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

d. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touchscreen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. The Internet is a global network of computers and other digital devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Seizure of Electronic Storage Devices: Based upon my knowledge, training and experience, and consultations with the Computer Analysis Response Team in the Federal Bureau of Investigation, I know that the search and seizure of information from digital devices often requires agents to seize most or all electronic storage devices (along

with related peripherals) to be searched later by a qualified expert in a laboratory or other controlled environment. This is true because of the volume of evidence contained on the digital devices and the technical requirements needed to properly search those devices.

18. The volume of evidence: Digital devices can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

19. Technical requirements: Searching digital devices for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since digital devices are extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

20. Procedures for Seizing Electronic Data: If specialists are available to assist with seizure of electronic data they will attempt to download all electronic data located in the vehicle at the time of the search. If this is not possible, it will be necessary to seize the digital devices from the site being searched and download the electronic data off-site.

21. Based upon my knowledge, training and experience, and consultation with the Computer Analysis Response Team in the Federal Bureau of Investigation, I know that searching digital devices for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because the peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as, all related instruction manuals or other documentation and data security devices.

22. This Affidavit seeks permission to locate not only electronically stored information on cellular phones and other electronic devices that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were to be used, the purpose of its use, who would use it, and when.

23. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

24. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of this Warrant.

25. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. Request to Move Computers, Mobile Phones, and Other Electronic Devices Off-Site to Search Before Return: In light of these concerns, I request permission to seize any computers, mobile phones, tablets, and electronic evidence that are believed to contain some or all of the evidence described in Attachment B, and to conduct an off-site search of these devices for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for the evidence.

27. Unlocking Devices with Biometric Features. This Warrant would permit law enforcement to compel SEMIEN or INDIVIDUAL 1 to unlock the electronic devices subject to seizure pursuant to this warrant using the devices' biometric features, if any. I seek this authority based on the following:

a. I know from my training and experience, as well as information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features, and the user of such devices can select which features they would like to use.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Once a fingerprint is registered, a user can unlock a device by pressing the relevant finger to the device's sensor, which is usually located at the bottom center of the device.

c. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this Affidavit, based on my training and experience, I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the

data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty

who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require SEMIEN or INDIVIDUAL 1 to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter an digital device that is subject to seizure pursuant to this Warrant and may be unlocked using one of the aforementioned biometric features, this Warrant would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of SEMIEN to the fingerprint scanner of the device(s) found in the **SUBJECT VEHICLE**; (2) hold the device(s) found in the **SUBJECT VEHICLE** in front of SEMIEN's face and activate the facial recognition feature; and/or (3) hold the device(s) found in the **SUBJECT VEHICLE** in front of SEMIEN's face to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this Warrant.

i. Due to the foregoing, if law enforcement personnel encounter an digital device that is subject to seizure pursuant to this Warrant and may be unlocked using one of the aforementioned biometric features, this Warrant would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of INDIVIDUAL 1 to the fingerprint scanner of the device(s) found in the **SUBJECT VEHICLE**; (2) hold the device(s) found in the **SUBJECT VEHICLE** in front of INDIVIDUAL 1's face and activate the facial recognition feature; and/or (3) hold the device(s) found in the **SUBJECT VEHICLE** in front of INDIVIDUAL 1's face to activate the iris recognition feature, for

the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this Warrant.

DNA EVIDENCE

28. Based on my training, experience, and conversations I have had with other law enforcement officials; I know that deoxyribonucleic acid (DNA) may be found in a person's saliva, blood, semen, hair follicles, and skin cells, among other places. I know that testable quantities of a person's DNA may often be found on objects that person has touched and clothes that person has worn. I know that testable quantities of a person's DNA can often be found in the vehicles a person has occupied and may also be found on items a person has been in physical contact with. I know that testable quantities of DNA are often transferred from one person to another during violent struggles, especially when one or both persons bleed during the interaction. I know that scientific experts can determine with relative certainty whether a particular person deposited a sample of DNA on a particular item by comparing that sample to a known sample collected directly from the person.

29. Items collected at the various scenes involved in this investigation, including the **SUBJECT VEHICLE**, will be tested for quantities of human genetic material. If testable DNA samples are obtained, analysts will compare them to known samples of DNA either to match a known contributor DNA profiles or rule out known samples as possible contributors.

30. Digital devices and DNA samples taken from the **SUBJECT VEHICLE** will be sent to a different location to be examined by experts at a later date.

31. Because the **SUBJECT VEHICLE** is in FBI's possession, this application seeks permission to execute the search at any time, day or night.

CONCLUSION

32. Based on the aforementioned information, I believe there is probable cause to believe that the **SUBJECT VEHICLE**, located at FBI Oklahoma City Headquarters, within the Western District of Oklahoma, including all digital devices therein, contain evidence of a crime, contraband, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime—specifically evidence of a violation of Title 18, United States Code, Sections 1111 and 1152.

33. Further, I believe the said evidence will be found when the attached warrant is executed. Consequently, based on the probable cause stated within this Affidavit, I specifically request authority to search and seize the evidence described above and in Attachment B hereto and incorporated herein by reference.

34. I, and/or any other duly authorized federal agent or forensic examiner, will execute the warrant requested above. Execution will include powering-up and turning-on devices, and may require authorities to employ techniques, including but not limited to, computer assisted scans of the entire medium, that might expose many parts of the device to human inspection to determine whether it is evidence described by the warrant.

FURTHER YOUR AFFIANT SAYETH NOT.

Jesse M. Stoda, Special Agent
Federal Bureau of Investigation

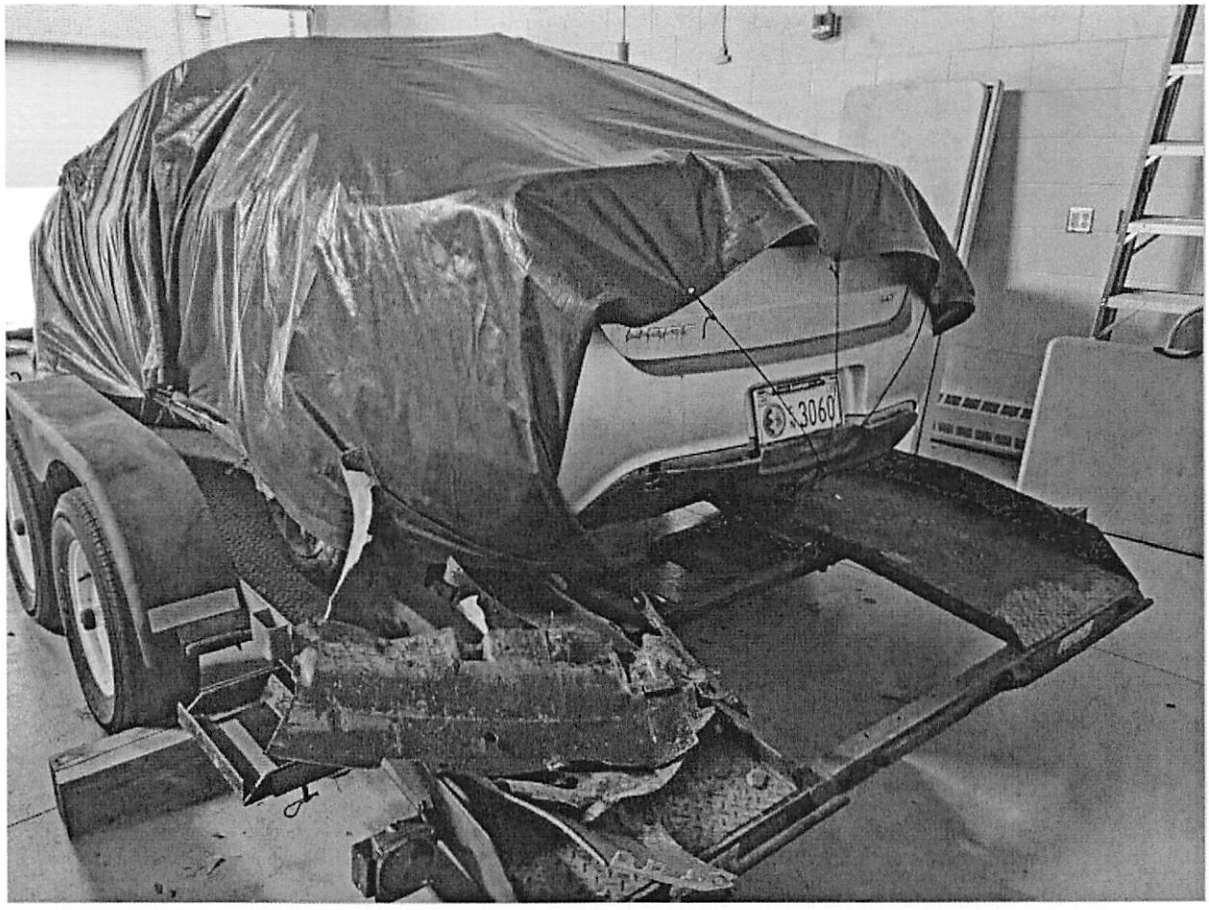
SUBSRIBED AND SWORN to before me this 7th day of June, 2023.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

A Silver Dodge Dart with Comanche Nation license plate CN3060 (the "**SUBJECT VEHICLE**"), which is currently located in the Western District of Oklahoma. The **SUBJECT VEHICLE** to be searched is described above and pictured below:



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 1111 and 1152:

1. Information, correspondence, records, documents, or other materials pertaining to circumstances surrounding the homicide of K.S.C., that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

    a. Cellular telephones, smartphones, tablets, personal digital assistants, computers, computer systems, computer hardware, computer software, tapes, cassettes, cartridges, streaming tape, commercial software, commercial hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems, and other computer related operation equipment;

    b. Any and all records of Internet usage including usernames and e-mail addresses and identities assumed for the purposes of communication on the Internet;

c. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;

d. Any and all personal effects in the **SUBJECT VEHICLE**; and

e. Computers or storage media used as a means to commit the violations described herein.

2. For any cellular device whose seizure is otherwise authorized by this warrant, and any cellular device that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "CELLULAR DEVICE"):

a. evidence of who used, owned, or controlled the CELLULAR DEVICE at the time the things described in this warrant were created, edited, or deleted;

b. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

c. evidence of programs (and associated data) that are designed to eliminate data from the CELLULAR DEVICE;

d. evidence of the times the CELLULAR DEVICE was used;

e. passwords, encryption keys, and other access devices that may be necessary to access the CELLULAR DEVICE;

f. documentation and manuals that may be necessary to access the CELLULAR DEVICE or to conduct a forensic examination of the CELLULAR DEVICE;

g. records of or information about Internet Protocol addresses used by the CELLULAR DEVICE;

h. records of or information about the CELLULAR DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

i. contextual information necessary to understand the evidence described in this Attachment.

3. All adapters, chargers, or other hardware necessary to charge the battery, or to maintain the functioning of, any of the equipment described above.

4. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the **SUBJECT VEHICLE**, including registration and insurance;

b. Records, information, and items relating to the ownership or use of computer equipment or cellular devices found in the **SUBJECT VEHICLE**, including sales receipts, bills, and handwritten notes;

c. Items used in the planning, commission, or concealment of the above-listed violations; and

d. Records and information relating to the identity or location of the persons suspected of violating the statutes described above.

5. Samples of biological material.

During the execution of the search of the **SUBJECT VEHICLE** described in Attachment A, law enforcement personnel are authorized to compel SEMIEN or INDIVIDUAL 1 to (1) press or swipe their fingers (including thumbs) to the fingerprint scanner of a device found in the **SUBJECT VEHICLE**; and/or (2) hold a device found in the **SUBJECT VEHICLE** in front of the face of SEMIEN or INDIVIDUAL 1, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, CD/DVDs, gaming systems, SIM cards, cellular phones capable of storage, memory cards, memory chips, and other magnetic or optical media.